UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:	)	
	)	Case No. 5:20-mj-49
The premises known as the offices of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 Account: pimpdaddyjohnboy@gmail.com	)	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251, 2252, 2252A	Possession or receipt of Child Pornography

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Applicant's signature

Michelle Pohlen, Special Agent Homeland Security Investigations
Printed name and title

Sworn to before me and:
☑ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 3-11-2020

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF: The premises known as the offices of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 Account: pimpdaddyjohnboy@gmail.com	CR 5:20-mj-49 **AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION**

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

I, Michelle Pohlen, Special Agent with Homeland Security Investigations (HSI), and currently assigned to the Rapid City, South Dakota Resident Agent in Charge (RAC) Office, being duly sworn, states as follows:

1. I have been a Special Agent (SA) with HSI since March 2019. In September 2019, I completed the Homeland Security Investigations Special Agent Training (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. In June 2019, I completed the Criminal Investigator Training Program (CITP), also located at FLETC in Glynco, GA. Prior to becoming a Special Agent, I was employed as a Federal Air Marshal with the Federal Air Marshal Service (FAMS) for two and a half years. Prior to FAMS, I served as a Police Officer with the Savannah Chatham Metropolitan Police Department (SCMPD) in Savannah, Georgia for one and a half years. I received a Bachelor of Arts degree in Law Enforcement in 2014.

2. During my law enforcement career, I have been involved in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I am aware that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of visual depictions of a minor engaging in sexually explicit conduct, using any means or facility of interstate or foreign commerce, including by computer or utilizing the internet.

4. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED

5. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a Google, Inc. account found during the investigation of an unknown subject utilizing the TARGET ACCOUNT, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), and which items are more specifically described in Attachment B. The specific Gmail account is: pimpdaddyjohnboy@gmail.com (also referred to in this affidavit as "Target Account").

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud-based storage service," as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18

U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide

computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. "Electronic Storage Device" includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

l. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and

uses separate control and data connections between the client and the server.

m. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

n. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1),

means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the

children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

b. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it

inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

e. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user's computer or external media in most cases.

8. Based on my training and experience and investigation in this case, I have learned the following about Google:

a. Google offers an e-mail service that is available free to Internet users called "Gmail." Stored electronic communications, including opened and unopened e-mail for Gmail subscribers may be located on Google's computers.

b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.

c. Subscribers can access their Gmail e-mail accounts by activating software on a device or computer, login in using unique usernames and passwords, and connecting to high-speed Internet computers called "servers" maintained and/or owned by Google. Subscribers also may be able to access their accounts from any other computer in the world through Google's web site on the Internet.

d. When a user sends any e-mail to a Gmail e-mail subscriber the email is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes it or until the stored e-mail exceeds the storage limit allowed by Google.

e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually through another subscriber's e-mail provider. Copies of sent e-mail are stored on Google's servers in the same manner as received e-mail, Google retains the email until the user

deletes it or exceeds the storage limit.

f. Even if the contents of the message no longer exist on the company's servers, Google may have records of when a subscriber logged into his or her account, when a message was sent or received, as well as technical routing information that law enforcement could use to determine who sent or received an e- mail.

9. From my training and experience, I am aware that Google's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

CYBERTIP 57151379

9. On 11/21/19, Det. Elliott Harding, Rapid City Police Department and ICAC, received CyberTip 57151379 from the National Center for Missing and Exploited Children (NCMEC), Dropbox reported child pornography. The CyberTip was eventually copied to compact disc and stored in ICAC evidence. Below is a summary of the information contained within the CyberTip:

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 10-13-2019 22:33:46 UTC
Description of Incident Time: The incident Date/Time is set to 24 hours before

the report was sent from Dropbox to NCMEC. For example, if we submit a report on "3/14/17 13:30", we will set the the incident Date/Time to "3/13/17 13:30.

Suspect

Email Address: pimpdaddyjohnboy@gmail.com (**SUBJECT ACCOUNT**) (Verified 09-04-2019 20:47:45 UTC)
Screen/User Name: Valo Appleseed
ESP User ID: 2469082384

IP Address: 2600:1014:b055:2036:b9e4:614:3618:2984 (Registration) 08-21-2019 21:20:42 UTC
IP Address: 2600:1014:b05d:1280:d974:2385:8ddd:9123 (Login) 09-04-2019 20:47:45 UTC
IP Address: 2600:1014:b05d:1280:d974:2385:8ddd:9123 (Login) 09-04-2019 20:48:07 UTC
IP Address: 2600:1014:b027:a520:d45e:a105:606d:c899 (Login) 09-05-2019 14:35:24 UTC
IP Address: 2600:1014:b02b:2c08:cd94:5106:dd48:a31e (Login) 09-09-2019 17:50:30 UTC
IP Address: 2001:48f8:1004:2eb:81d5:4de:4fef:5edc (Login) 09-10-2019 12:25:08 UTC
IP Address: 2600:1014:b06f:2814:15c7:4b33:715f:c5cf (Login) 09-10-2019 19:14:47 UTC
IP Address: 2600:1014:b06f:b3e0:463:644d:db8e:d18 (Login) 09-11-2019 15:24:23 UTC
IP Address: 2600:1014:b06f:b3e0:463:644d:db8e:d18 (Login) 09-11-2019 17:04:03 UTC
IP Address: 2600:1014:b012:ba1b:bcb1:560:75fb:7fe5 (Login) 09-12-2019 14:03:23 UTC
IP Address: 2600:1014:b012:ba1b:bcb1:560:75fb:7fe5 (Login) 09-13-2019 16:58:02 UTC
IP Address: 2600:1014:b060:5062:fc3e:3629:fefb:bf75 (Login) 09-17-2019 18:52:45 UTC
IP Address: 2600:1014:b014:2914:a4ba:d321:567f:d5d (Login) 10-01-2019 18:35:04 UTC

Detective Note: The IP addresses above, per Maxmind.com, came back to Verizon Wireless with the exception of IP address 2001:48f8:1004:2eb:81d5:4de:4fef:5edc which came back to Midco.

Uploaded File Information
Number of uploaded files: 3

10. Det. Harding made the following observations of the images included in the Cybertip:

RUSAdel.mp4

Harding observed video RUSAdel.mp4. The video was 18 min. 16 seconds in length. The video showed a girl approximately 13-15 years of age wearing blue jeans, a blue shirt with pink writing on the front, a cross necklace and shorter dark hair. In the background, Harding could see light colored vertical line print wallpaper and an electrical outlet. He could also see a pink sheet toward the bottom of the screen. The girl danced for the video camera. The girl then walked through what appeared to be a house, but the background was blurry to note any details. The girl stopped in another room with a dark door and what appeared to be towels and clothes hanging in the background. Harding could see a partial window in the background with light green curtains. The girl appeared to be communicating with someone on the device she was using to record herself and receiving direction. The girl pulled down her underwear twice and each time Harding could see her nude vagina. The girl removed her underwear, danced for the video camera and exposed her nude vagina and anus. The girl rubbed both her nude anus and vagina with her finger.

SaSHA.mp4

Det. Harding observed video SaSHA.mp4. The video was 17 min. 44 seconds in length. The video showed a girl approximately 10-12 years of age with long blond hair. He could see multicolored curtains and bed sheet in the background. The girl rubbed her nude breast area, which was visible. The girl sucked her finger and rubbed her nude nipples. The girl removed her underwear exposing her nude vagina. The girl rubbed her nude vagina as well as inserted her finger. The girl spread apart the lips of her vagina for the video camera. Harding could hear a foreign voice whisper, but could not tell if it was a boy or girl. He could not tell if the person whispering was the girl in the video. The girl held up her first finger toward the end of the video. It appeared as if she was communicating with someone.

uploadlog.csv

Det. Harding reviewed file uploadlog.csv provided within the CyberTip. The file uploadlog.csv was unable to be uploaded to the case report. Below is the contents of the file:

timestamp	user	action	path

8/21/2019 23:49	2469082384	ADD	/Things/bonus floetry 22/SaSHA.mp
8/21/2019 23:49	2469082384	ADD	/Things/bonus floetry 22/RUSAdel.m

According to the uploadlog.csv file, the two videos mentioned above were added to the Dropbox account in question on 8/21/19 at 23:49 hours, specifically the folder /Things/bonus floetry 22/

IDENTIFYING VALO APPLESEED ESP

11. On 1/13/20, Det. Harding sent an email to HSI Analyst Amber Cooper requesting she attempt to identify Valo Appleseed. On January 13, 2020, Analyst Cooper sent a customs summons to Google for pimpdaddyjohnboy@gmail.com. On January 30, 2020, Google responded in part with the following information:

Google Account ID: 313633324244

Name: John Klingman

E-Mail: pimpdaddyjohnboy@gmail.com **(SUBJECT ACCOUNT)**

Created On: 2013-02-21 18:42:46 UTC

Recovery Email: pimpdaddyjohnboy@hotmail.com **(SUBJECT ACCOUNT)**

12. On January 13, 2020, Analyst Cooper sent a customs summons to Midcontinent Communications for the IPv6s 2001:48f8:1004:2eb:81d5:4de:4fef:5edc on 09-10-2019 @ 12:25:08 UTC. Midcontinent Communications responded in part with the following information:

Brandie Blosser

507 Cardinal CT

Box Elder SD 57719

Home Phone: 605-391-0647

13. On January 13, 2020, Analyst Cooper sent a customs summons to Verizon Wireless for 2600:1014:b055:2036: b9e4:614:3618:2984 on 08-21-2019@ 21:20:42 UTC, 2600:1014:b060:5062:fc3e:3629:fefb:bf75 on 09-172019@ 18:52:45 UTC, and 2600:1014:b014:2914:a4ba:d321:567f:d5d on 10-01-2019@ 18:35:04 UTC. On January 22, 2020, Verizon responded in part with the following information:

Business Name: Black Hills Works Inc.

Address: 3650 Range Road, Rapid City, SD 57702

Contact: Kathy Staton

*There are approximately 56 other phone numbers associated to this account.

14. Analyst Cooper learned that in a September issue of the Black Hills Works Inc.'s Monthly publication contained an article thanking John Klingman for 7 years working for the company. His name is listed on page 7 of the article.

15. Analyst Cooper conducted a law enforcement inquiry on 507 Cardinal CT, Box Elder, SD 57719. Some subjects associated to the address include:

Brandie K Blosser DOB: 02/1988 Spouse: Derek

Bradley J. Halvorson DOB: 11/29/1994

John Klingman DOB: 10/07/1990

16. On January 15, 2020, Analyst Cooper sent a preservation to Dropbox for the Email Address pimpdaddyjohnboy@gmail.com, Screen/User

Name: Valo Appleseed, and ESP User ID: 2469082384.

17. A law enforcement inquiry showed John Klingman (10/07/1990) associated with 507 Cardinal Ct., Box Elder, SD 57719. Local police records confirmed this as well.

CYBERTIP 61787646

18. On 2/28/20, Det. Harding received CyberTip 61787646 from the National Center for Missing and Exploited Children (NCMEC). Dropbox reported child pornography to NCMEC. Harding made a copy of the CyberTip to compact disc and stored it in ICAC evidence. Below is a summary of the information contained within the CyberTipL

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 12-25-2019 21:41:51 UTC
Description of Incident Time: The incident Date/Time is set to 24 hours before the report was sent from Dropbox to NCMEC. For example, if we submit a report on "3/14/17 13:30", we will set the incident Date/Time to "3/13/17 13:30

Suspect
Email Address: vvalo6969@gmail.com (Verified 09-17-2019 14:35:54 UTC)
Screen/User Name: Valo Appleseed
ESP User ID: 2532546960
IP Address: 2600:1014:b012:ba1b:bcb1:560:75fb:7fe5 (Registration)
09-12-2019 13:55:48 UTC
IP Address: 2001:48f8:1004:2eb:d1a8:8e1:6975:d41a (Login)
09-13-2019 16:22:07 UTC
IP Address: 2001:48f8:1004:2eb:5ce4:1a72:f79e:ad8c (Login)
09-17-2019 12:48:03 UTC
IP Address: 2001:48f8:1004:2eb:a92f:cf89:d5a9:32b8 (Login)
09-26-2019 22:15:27 UTC
IP Address: 2600:1014:b014:2914:a4ba:d321:567f:d5d (Login)
10-01-2019 18:24:46 UTC

IP Address: 2600:1014:b04e:8f3d:49c2:6303:600a:760f (Login)
10-25-2019 10:20:12 UTC
IP Address: 2600:1014:b04e:8f3d:49c2:6303:600a:760f (Login)
10-25-2019 10:33:15 UTC
IP Address: 2600:1014:b04e:8f3d:49c2:6303:600a:760f (Login)
10-25-2019 15:24:41 UTC
IP Address: 2600:1014:b04e:8f3d:49c2:6303:600a:760f (Login)
10-27-2019 17:12:04 UTC
IP Address: 2600:1014:b04e:8f3d:a82b:677b:cb8:84f4 (Login)
10-29-2019 12:24:23 UTC
IP Address: 2600:1014:b04e:8f3d:a82b:677b:cb8:84f4 (Login)
10-30-2019 20:41:14 UTC
IP Address: 2600:1014:b041:6860:6de7:c028:c604:9e50 (Login)
10-30-2019 22:04:21 UTC

19. Several of the IP addresses associated with the second Cybertip are the same as those connected to John Klingman in the first Cybertip.

Additional Information Submitted by the Reporting ESP
Dropbox records are kept in GMT unless otherwise noted.

CHILD PORNOGRAPHY OBSERVATIONS

20. Det. Harding viewed video iVPyum13.mp4. The video was 5 seconds in length. The video showed a child of unknown sex, approximately 3-5 years of age, being orally raped. The video showed what appeared to be an adult male with his nude penis in the child's mouth. The male then said, "Ready." The child responded in the negative due to not being able to talk because of the penis. The male, holding the child's head, moved the child's mouth along his penis. The child was heard gagging twice. The child had shoulder length blond hair and a red flannel long sleeved button shirt.

21. Dropbox provided the file uploadlog.csv. Upon reviewing the .csv file, Det. Harding learned iVPyum13.mp4 was added to the suspect Dropbox account folder /Things2/vids@/1/ on 10/31/2019 2:39:52 PM.

PRESERVATION: DROPBOX AND GMAIL

22. On 2/28/20, Det. Harding requested HSI Analyst Amber Cooper to preserve the suspect Dropbox account and associated Gmail account vvalo6969@gmail.com.

SUBPOENA: GMAIL

23. On 2/28/20, Det. Harding requested HSI Analyst Amber Cooper to subpoena Gmail account vvalo6969@gmail.com. As of the writing of this affidavit, Det. Harding has not received subpoena return information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

24. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

25. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a "district court of the United States (including a magistrate judge of such court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

26. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the following account: pimpdaddyjohnboy@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Google, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Google, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Google, Inc. not to notify the user of the existence of this warrant.

REQUEST FOR SEALING OF MATTER

27. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

28. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

29. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Google, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Google, Inc. account, listed in Attachment A has been used for the exploitation of children using the internet including violations of 18 U.S.C. § 2422(b) (enticement of a minor using the internet), which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Gmail account, exploited minors using the internet

and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this warrant affidavit. The account is pimpdaddyjohnboy@gmail.com.

40. Law enforcement agents will serve the warrant on Google, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

41. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Google, Inc. via the internet and to allow Google, Inc. to copy the data outside of this agent's presence.

RETURN COMPLIANCE BY GOOGLE, INC.

42. Google's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, Google requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

Dated: 03/11/2020

Special Agent Michelle Pohlen
Department of Homeland Security
Investigations

Sworn to before me and:
☑ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

this 11th day of March, 2020

Daneta Wollmann
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the following Gmail email account, under an account known to be stored at the premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043: pimpdaddyjohnboy@gmail.com.

ATTACHMENT B
Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Google, Inc. (the "Provider") to facilitate execution of the warrant:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google Inc., including any emails, records, files, logs, or information that have been deleted but are still available to Google Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 28, 2020. Google Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in the email account which is helpful to determine the accounts' user's or owner's true identity:

a. The contents of all e-mails associated with the account, from the time of the account's creation to the present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each e-mail;

b. The contents of all Instant Messages (IM) associated with the account, from the time of account's creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP addresses used to register the account, all log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of services utilized;

e. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between Google Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. §§ 2252, and 2252A, receipt, distribution and possession of child pornography, including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;

b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;

c. Any person knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged, or attempting to do so;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the email account owner or user;

e. Evidence indicating the email account users or owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers listed on Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier listed on Attachment A and other associated accounts.

III. Information Regarding Search Warrant Compliance by Google:

Google shall disclose responsive data, if any, by sending to:

Special Agent Michelle Pohlen
Department of Homeland Security Investigations
1516 Fountain Plaza Drive
Rapid City, SD 57702
Michelle.A.Pohlen@ice.dhs.gov

Google shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252A or similar statute or code. In the alternative, Google may make the responsive data available to Special Agent Pohlen by use of its law enforcement website.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11) & (13)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google Inc., and my official title is _____. I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and

c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rules 902(11) and (13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:

The premises known as the offices of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 Account: pimpdaddyjohnboy@gmail.com	)	Case No. 5:20-mj-49

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota *(identify the person or describe the property to be searched and give its location)*:

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, 2252A, as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 25, 2020 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)*. ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 3-11-2020 2pm

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

CC: AUSA Collins + Agent

Return

Case No.: 5:20-mj-49	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title